Visa Business News

Data Security

10 October 2019

# What To Do If Compromised Document Revised

**AP, Canada, CEMEA, LAC, U.S.** | *Acquirers, Issuers, Processors, Agents*

***Visa Network***

**Overview:** Visa's *What To Do If Compromised* document has been updated to more clearly define required procedures and timelines for reporting and responding to a suspected or confirmed account data compromise. This latest version incorporates new investigation fees and non-compliance assessment information. Fees are entirely avoidable if entities cooperate with applicable investigations in a timely fashion.

## Protecting Payment Card Data

Visa is committed to proactively identifying and investigating all threats and account data compromises affecting the payment ecosystem. To that end, Visa works to ensure the timely resolution of external data compromise events, drive notification of at-risk accounts to stem fraud impacts, and synthesize forensic evidence, intelligence, and fraud analysis to formulate remediation plans that strengthen payment system security.

Full cooperation during data breach events can help to contain and mitigate the breach event more quickly and help minimize the resulting fraud affecting Visa clients. Any entity that stores, processes, or transmits payment card data or has access to those systems or data is required to adhere to and maintain compliance with all Payment Card Industry Data Security Standard (PCI DSS) requirements.

**Mark Your Calendar:**

- Webinar: Data Compromise Event Reporting and Management **(23 October 2019)**
- Investigation fees and NCAs take effect in the AP, CEMEA, LAC and U.S. regions **(18 April 2020)**
- Investigation fees and NCAs take effect in Canada **(18 July 2020)**

**Related Training From Visa Business School:**

- Risk

Entities that suspect or have confirmed a compromise event of their payment systems, or payment systems they service or support, **must** take prompt action per the *What to Do If Compromised* (WTDIC) guide to prevent additional exposure.

## Responding to a Suspected or Confirmed Account Data Compromise

Visa's WTDIC document is a supplement of the Visa Rules and applies to entities that suspect or have experienced a compromise event of their payment systems, or payment systems they service or support. This includes, but is not limited to, all Visa member financial institutions (i.e., issuers and acquirers), merchants, processors, gateways, agents, service providers, third party vendors, integrator resellers and other entities, as well as other payment system participants operating or accessing the payments environment.

Version 6.0 of Visa's WTDIC, **effective 19 October 2019**, establishes procedures and specific timelines for reporting and responding to a suspected or confirmed account data compromise event. To mitigate payment

system risk during a compromise event, prompt action is required to prevent additional exposure, including ensuring containment actions and remediation, such as ensuring that proper PCI DSS and PCI PIN Security controls are in place and are functioning correctly. Visa's updated WTDIC document will guide clients and entities through critical, required compromise event components and procedures that include:

- Providing notification to Visa
- Conducting an initial investigation and providing an incident report to Visa
- Providing exposed payment account data to Visa
- Managing PCI Forensic Investigation / Independent Investigation as required
- Complying with all client requirements for suspected or confirmed compromise events
- Following eCommerce Threat Disruption (eTD) requirements
- Understanding potential impacts of investigation fees and non-compliance assessments (NCAs)

## New Investigation Fees

Visa aims to ensure the timely resolution of compromise events and drive notification of at-risk accounts to stem fraud impacts.

In support of these objectives, **effective 18 April 2020** in the AP, CEMEA, LAC and U.S. regions and **effective 18 July 2020** in Canada, Visa is introducing investigation fees to encourage entities to cooperate throughout each phase of the investigation process.

Visa's WTDIC document specifies the investigation fees and how they are assessed. Fees are entirely avoidable if entities cooperate in a timely fashion.

**Note:** Investigation fees will apply in the AP, Canada, CEMEA, LAC and U.S. regions.

## Non-Compliance Assessments

NCAs go into effect **18 April 2020** in the AP, CEMEA, LAC and U.S. regions and **18 July 2020** in the Canada region. The assessments are designed to deter entities from failing to comply with the required procedures and timelines for reporting and responding to a suspected or confirmed compromise event.

## Upcoming Webinar Presentations

A Data Compromise Event Reporting and Management webinar will be presented at the following times on Wednesday, 23 October 2019:

- 8 a.m. Pacific time
- 8 p.m. Pacific time

## For More Information

Merchants and third party agents should contact their acquirer.